2019-09-11-A Aries Working Group Call (US morning)

Summary:

- The right place to create an Anoncreds library: shared libraries export C-callable API, but the language doesn't matter (C, Rust, Go)
- Aries-Framework-Go has a Verifiable Credential package that could be made available to other frameworks
- Building a generic DIDDoc parser
- Aries-Wallet is probably the right shared library to build first

Note: This call is Recorded. Recordings posted at the bottom of the page.

Date
11 Sep 2019 (7AM Los Angeles, 10AM New York, 3PM London, 17H Moscow)

Remember the Hyperledger Code of Conduct

Anti-Trust Policy:

Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

Attendees

- Name (organization) <email>
  - John Callahan (Veridium) <jcallahan@veridiumid.com>
  - Ken Ebert (Sovrin Foundation) <ken@sovrin.org>
  - Richard Esplin (Evernym)
  - Samuel Smith (ProSapien) <sam@samuelsmith.org>
  - Troy Ronda (SecureKey) <troy.ronda@securekey.com>
  - Stephen Curran (Cloud Compass/BC Gov) <swcurran@cloudcompass.ca>
  - Mike Lodder (Sovrin Foundation) <mike@sovrin.org>
  - Rebecca Christman <rebeccachristman@gmail.com>

Welcome / Introductions

Announcements

- Community project: Aries RFCs - process to move HIPES; RFCs that have been moved concepts / features / pull requests.
- Aries Workshop/Connectathon December 3-5 in Provo, Utah (details to follow)
- IIW
- Hyperledger Maintainers Conference: Minneapolis in October.
- Bootcamp Russia: Event Location

Summary of Prior Calls and Related Meetings

- Aries WG
- Indy
- Ursa
  - Question for the Indy team on testing and deploying debian packages

Release Status

- Aries-CloudAgent-Python (bc.gov) - Release 0.3.2 has been tagged and is on PyPi
  - Support for RFC 0036 and RFC 0037 Credential Exchange protocols, 0.1 version of those protocols deprecated
  - Working on next release, particularly on revocation support.
- Aries-Framework-Go (Troy)
  - First milestone: Framework Go v0.1.0
  - Weekly planning notes
- Aries-SDK-Ruby (Jack)
  - Released as a Gem (0.0.3) due to Rails 6 issues
  - Developed docker image with Rails 6 (Ruby 2.5.1) with Indy-SDK to test Aries-SDK-Ruby via Dokku deployment
- Needed for exploring concurrency and compatibility issues with Sidekiq, Resque, SuckerPunch, etc.

- Aries-Framework-DotNet (Tomislav)
  - Moved from StreetCred to Aries: https://github.com/hyperledger/aries-framework-dotnet

- Aries-StaticAgent-Python - Release 0.4.0
  - Move from Pysodium PyNaCl
  - Improved module interface and routing.

- Aries-SDK-Python - Wrapper from JeromK and SBCA?

- Aries-SDK-Java
  - Aries-SDK subchannel / discussion aries-sdk-java

- Aries-SDK-JavaScript
  - People are collaborating in the repo.

- Indy
- Ursa

  - Working on release of 0.2.0 (September / October)
    - ZKP / ZKLang improvements
    - Debian packages
    - Refactor internal plumbing for anoncreds 2.0, shouldn't impact external interfaces
    - Refactor multi-signature BLS in addition to aggregated signature

  - Sovrin Foundation is looking to build a Indy specific Ursa, with ZKPs. Other Aries clients would build a different Ursa.

**Work Updates**

- Rich Schemas and W3C Verifiable Credentials (Ken)
  - Working on context object in Node. PR for Indy-Node is almost ready for review.
  - Making progress on the new schema object.
  - In order to do the review, need new Indy HIPES: each new object, the new flow for creating credentials, creation of presentation request and presentation, compatibility with the old credential format

- SDK 2.0 architecture / Indy-Aries split (Sergey)
  - http://jira.hyperledger.org/browse/IS-1285
  - https://docs.google.com/document/d/1MYMi4NkixfoIjeC79WBOXQ_AQ3_9rG-iK3IzAs6vR0/edit#heading=h.z1u0dzf62oi POA and discussion
  - https://docs.google.com/drawings/d/1d-aCRC_Nzyyw9nyQif9_vBGbeWhp69M4T5_b_ytAI/edit?usp=sharing Indy SDK Migration box diagram

- https://docs.google.com/drawings/d/1sUffkRPlufingeeRjjBniVt9Ek3CNih9IUqym8mU4M/edit?usp=sharing Aries Architecture
  - https://hackmd.io/_BhJewTlSUqMGNDc4SvgNw?edit developing ideas around APIs

- Aries Presentations
  - https://hackmd.io/@qjPgYQjMT3azdpSAFgo5PA/HylVdhVGr Daniel B's proposal for separating wallet and crypto
  - https://docs.google.com/document/d/18kHgTsHk5W9cakbmpv8rxKzXNhWhc7hHnXGyxkl/edit# Daniel H's analysis of challenges and approaches

- Architecture of Aries Verifiable Credentials Proof Formats
  - Boundary between the claim type and the signature type
  - Where should it live? Anoncreds (ZKP)s, JWTs, Link Data Signatures

- Aries Anoncreds Framework

**RFC Progress**

**Other Business**

- Aries shared libraries export their API as C-callable, but the implementation language doesn't matter: C, Rust, Go
- DIDDoc parser in Rust:
  - https://crates.io/crates/did_doc
  - https://github.com/dhuseby/did

- What is the next step we can take:
  - Richard's proposal for order of work
    - Move Indy-SDK into Aries-Core (October release)
    - Split out wallet into Aries-Wallet (November release)
    - Define the resolver interface (November effort)
    - Split out resolver into Indy-Resolver (December release)

- Questions
  - Iterative approach: do something that we can improve on.
    - Start with the needs of the agents (Aries-Cloud-Agent) and build the Aries core architecture from that.
    - Maintain Indy-SDK alongside Aries-Core / Aries-Wallet / Aries-Resolver?
    - Who will be the maintainers of the new libraries? Do we want cross-organization PR reviews?
    - Best way to maintain history, and make the reorg transparent
      - History continues public in Indy-SDK, so might be better to start clean in Aries
      - concerns with old DCO process: can use Mike Lodder's approach he used for movingindy-crypto to ursa
    - What to do with the Indy CLI?
    - CI / CD in Jenkins or GitLab?

- Daniel's proposal for order of work
  - Split out Indy wallet into Aries-Wallet
  - Define the resolver interface and create the resolver libraries (indy and peer)
    - The peer DID resolver isn't dependent on other libraries https://github.com/dhh1128/pypeerdid
  - Wait on Aries-Core

- Architecture of Aries core library
What is our fastest path to a library that framework implementors could consider using?
Daniel's analysis of Aries API Surfaces [link]
Background in previous meetings: July 31, August 14
Progress of Ken's POC
Key questions: [link]

Future Topics
- Next call
- Other:
  - Hubs vs Agents
  - Payments in Aries
  - wallet query language
  - IOT best practices (Robert Mitwicki, Adam Burdett, Lohan Spies)
  - DID Resolution W3C and Sam's concerns: [link]

Action items
- Schedule a deep dive into Aries / Indy architecture (Ken / Richard)

Call Recording

<table>
<thead>
<tr>
<th>File</th>
<th>Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multimedia File GMT20190911-140155_Community_1494x1080.mp4</td>
<td>Sep 11, 2019 by Richard Esplin</td>
</tr>
</tbody>
</table>